

FACTORIZING PATH GENERALIZED ALGORITHM WITH PERFECT SQUARES WITHIN PRECINCTS OF $6k \pm 1$ FORMS

Eng. Rosario Turco, Dr Michele Nardelli, Prof. Giovanni Di Maria, P.a. Francesco Di Noto, Prof. Annarita Tulumello, Prof. Maria Colonnese.

ABSTRACT

This article is a further study of previous work “Primality test, Factoring and $\pi(N)$ with $6k \pm 1$ forms” (see reference [1]). Present work shows as, within precincts factoring with $6k \pm 1$ forms, we can introduce a generalized algorithm to confront all types of perfect squares: Pythagorean’s triads, perfect squares for number with distance 2 (both twin prime numbers and not ones) or perfect squares with a greater distance of 2.

In this occasion, we insert a new theorem on this argument, that permits to solve, with an efficient algorithm, the problem.

Introduction (preliminary remark)

In [1] we presented the forms $6k \pm 1$ and their properties and defined a Primality Theorem with a Factoring Theorem. In this work, standing factoring technique already explained in [1], we will confront the possibility, instead, to generalize, within precincts of factoring algorithm, the perfect squares’ technique, so it goes well: not only, as in [1], for twin prime numbers, and not numbers greater than of 2 (numbers at distance 2, for example 5 and 7) but also for Pythagorean’s triads and numbers (primes or not) greater than of 2 (for example 11 and 17).

Now we define an our Factoring Theorem named QGP.

Factoring Theorem QPG (Generalized Perfect Squares):

Let P a positive integer. If exists a pair of values (Q' , Q) both perfect squares or also constituent with P a Pythagorean triads, such as $P + Q' = Q$ with $Q > P$, then P is decomposable in a product in the following way:

$$P = (\sqrt{Q} - \sqrt{Q'}) * (\sqrt{Q} + \sqrt{Q'}) \quad (1)$$

If in the (1) the term $\sqrt{Q} - \sqrt{Q'} = 1$, it is useless to factorize in factors P in this way; while is unseemly, in terms of factoring’s speed, the look for a pair (Q, Q’) if within precincts of search of the pair the term Q has become greater of P.

The method consists to search, therefore, a Q’ perfect square that, added to P, provides another perfect square Q.

Let’s go seeing some explanatory examples.

Example 1 (P even compound with factor at distance 4)

$$P = 60 \quad P < Q: Q = 64 \quad Q' = 4 < P, \quad \sqrt{Q} = 8, \quad \sqrt{Q'} = 2, \quad P = (8-2)*(8+2) = 6*10$$

Example 2 (P odd compound with prime numbers at distance 4)

$$P = 77 \quad P < Q: Q = 81, \quad Q' = 4 < P, \quad \sqrt{Q} = 9, \quad \sqrt{Q'} = 2, \quad P = (9-2)*(9+2) = 7*11$$

Example 3 (P odd compound with prime numbers at distance 2 or twin prime numbers)

$$P = 35 \quad P < Q : Q = 36, Q' = 1 < P, \sqrt{Q} = 6, \sqrt{Q'} = 1, P = (6-1)*(6+1) = 5*7$$

Example 4 (P odd compound with a Pythagorean's triads)

$$P = 9 \quad P < Q : Q = 25, Q' = 16 < P, \sqrt{Q} = 5, \sqrt{Q'} = 4, P = (5-4)*(5+4) = 1*9$$

It's useless to use this method because the difference of roots giveback 1 in this case.

Example 5 (P = prime number)

If we continue without to stop when $Q' > P$, we will obtain:

$$P = 17 \quad P < Q : Q = 81, Q' = 64 < P, \sqrt{Q} = 9, \sqrt{Q'} = 8, P = (9-8)*(9+8) = 1*17$$

We stop before because $Q' > P$.

On the other hand, for prime numbers, if we go on, the method whatever is not apply in this case, as in the previous one (roots difference). In other terms the method, in general, stop oneself because the search of pair (Q', Q) is not any more considered advantageous, in two possible cases:

- roots ' difference = 1
- $Q' > P$

In both cases the number is not considered a number to factorize with perfect square method: it could be a compound or a prime number but for breaking up it in factors and his primality we prefer to apply a faster technique, the "second step", after the control of perfect square, described in [1].

We can easily observe that all prime numbers have root's difference equivalent to 1 with $Q' < P$.

This may be a signal of prime number, but we prefer to come out before, instead, to prove many values Q' , this in the point of view to return more fast the decomposition.

Examples: $23 + 121 = 144$, $129 + 196 = 225$, etc.

The compound numbers present, often, also them root's difference equivalent to 1 but already to $Q' < P$ (since we stop at the first that we find), and they are characterized, as far as compound numbers, to have more solutions about the equation $P + Q' = Q$. Also here the difference 1 and $Q' < P$ could be as a signal of compound number.

Example $21 + 4 = 25$ but also $21 + 100 = 125$.

Additional condition.

Obviously in the cycle's search of solution, no terms of [1] will be greater or equivalent to P. We come out from cycle if we violate this condition.

Algorithm

The Theorem provides a criterion of suitable stop or a criterion not suitable to use generalized technique of perfect square. In every case the Theorem permits a faster algorithm compared to [1], because with equivalence of steps, two steps: one of perfect square's control and other to factorize without perfect square, now in "step of perfect square control" we try distances between the numbers (Pythagorean's triads, perfect squares for number with distance 2 and with distance greater than 2). In the INFORMATIC APPENDIX we present the algorithm above discussed, presented in source quadrpGen.c, but integrated within precincts of factoring instead of Source quadrp.c presented in [1].

References

[1] Test of primality, factoring, and $\pi(N)$ with $6k \pm 1$ forms. Eng. Rosario Turco, Dr. Michele Nardelli, prof. Giovanni Di Maria, P.a. Francesco Di Noto, prof. Annarita Tulumello - CNR Solar.

- <http://www.gruppoeratostene.netandgo.eu> Gruppo Eratostene
- <http://xoomer.alice.it/stringtheory/Home.html> Michele Nardelli
- <http://www.geocities.com/SiliconValley/Port/3264> R.Turco - Aladdin's Lamp (sezione MISC).